Committee on National Security Systems

CNSSP No. 17
January 2014

POLICY

ON

WIRELESS SYSTEMS

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE
FURTHER IMPLEMENTATION

CHAIR

FOREWORD

1. The Committee on National Security Systems (CNSS) is issuing this policy directing agencies to safeguard national security systems (NSS) when using wireless technologies.

2. This policy supersedes the Committee on National Security Systems Policy (CNSSP) No. 17, *National Information Assurance (IA) Policy on Wireless Capabilities*, May 2010.

3. The heads of D/A are ultimately responsible for protecting NSS (both unclassified and classified) that transmit, receive, process, or store information using wireless technologies. D/A shall ensure that all wireless NSS and their components, to include new acquisitions, legacy systems, and upgrades, comply with this policy.

4. The CNSS has the authority to request the information and technical support necessary from the heads of D/As to ensure that NSS meet the minimum requirements set forth in this policy, and will review and assess D/As wireless NSS communications programs for compliance in accordance with CNSSD 900, *Committee on National Security Systems (CNSS) Governing and Operating Procedures*, (Reference a).

5. This policy is available from the CNSS Secretariat, as noted below, or the CNSS website: www.cnss.gov.

/s/

TERESA M. TAKAI

CNSS Secretariat (IE32)
National Security Agency * 9800 Savage Road * Suite 6716 * Ft. Meade MD 20755-6716
cnss@nsa.gov

POLICY ON WIRELESS SYSTEMS

SECTION I – PURPOSE

1. This policy also assigns responsibilities for improving the security posture of the U.S. Government Executive Departments and Agencies (D/As), and provides references for a minimum set of security measures required for the use of wireless technologies in a national security environment. For this policy, the term D/As shall be interpreted to include Federal bureaus and offices.

SECTION II – AUTHORITY

2. The authority to issue this Policy derives from National Security Directive (NSD) 42, (Reference b), *National Policy for the Security of National Security Telecommunications and Information Systems*, which outlines the roles and responsibilities for securing national security systems, consistent with applicable law, Executive Order 12333, (Reference c), as amended; and other Presidential directives.

3. Nothing in this Policy alters or supersedes the authorities of the Director of National Intelligence.

SECTION III – SCOPE

4. This policy applies to all D/As employees, contractors, and visitors that use or plan to use, implement, or test wireless technologies on or in proximity to national security systems (NSS). It also applies to the processes that enable the D/As to oversee the planning, design, development, acquisition, implementation, upgrade, use, control, operation, maintenance, and disposition of existing and future NSS wireless capabilities within their scope of authority.

SECTION IV – POLICY

5. Procurement of commercial wireless technologies and systems shall comply with the relevant National Information Assurance Partnership (NIAP) Common Criteria Protection Profiles in accordance with CNSS Policy No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products* (Reference e). This applies to all commercial IA and IA-enabled IT products.

6. The following requirements shall be incorporated into D/As NSS programs where wireless technologies are used to transmit, receive, or process information on NSS or in proximity to NSS. In addition, D/As are encouraged to review the Best Practices in Annex B when implementing and operating a wireless system.

a. TEMPEST countermeasure requirements reviews shall be completed in accordance with CNSS Policy No. 300, *National Policy on Control of Compromising Emanations* (Reference f) and CNSS Instruction No. 7000, *Tempest Countermeasures for Facilities* (Reference g) prior to acquiring wireless NSS solutions for use on or within proximity to an NSS.

b. At a minimum, D/As shall issue policies that include, or incorporate into existing policies, the following management controls:

    1) When integrating wireless devices, services, and technologies into NSS, D/As shall implement a risk management process that adheres to the guidelines found in CNSS Policy No. 22, *Information Assurance Risk Management Policy for National Security Systems* (Reference h) and the principles set forth in National Security Decision Directive 298, *National Operations Security Program* (Reference i).

    2) The procurement of wireless technologies for use on or with NSS shall be prohibited unless a risk assessment consistent with CNSSD 505, *Supply Chain Risk Management (SCRM)* (Reference j), is completed and accepted by the AO (this excludes the procurement of wireless technologies for tests, pilots, prototypes, and feasibility studies for use on non-operational networks or networks used primarily for research purposes).

    3) Where technically feasible, procure wireless technologies that support hardware and/or firmware integrity validation and trusted root(s), in accordance with NIST SP 800-147, *BIOS Protection Guidelines* (Reference k) and NIST SP 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices* (Reference l), respectively.

    4) Wireless risk assessments shall address the protection of NSS from the point of origin; during transmission; when received; while processing on wireless technology; and when using a wireless system as the sole or principal system for meeting critical or primary mission essential functions.

    5) A configuration baseline shall be established that defines the organization's minimum requirements for compliance with this policy, and ensures that wireless technologies, network access points, and documentation are adequate to protect NSS and the information therein. In those instances where a D/A has an existing Information Technology Configuration Control Board (ITCCB) for NSS; the ITCCB shall incorporate the wireless requirements referenced above.

6) All NSS that employ wireless technologies used for transmission, receipt, processing, and storage shall complete a security control assessment and be granted an authorization to operate by the D/A AO prior to transmitting, receiving, processing, or storing data.

7) Continuous monitoring shall be employed in support of:

   a) Operational risk assessments of information systems and networks;

   b) Network management (to include monitoring of network traffic, network faults, network performance, bandwidth consumption, and routing); and

   c) Computer Network Defense and Intrusion Detection.

   d) At a minimum, annual inspections in support of risk assessments shall be performed to identify deviations from the D/A-approved configuration baseline of NSS employing wireless technologies. All deviations shall be documented and reported to the AO and CSA.

8) Where practicable, wireless technologies employed on NSS shall support interoperability through the adoption of commercially available, standards-based products, technologies, and services in accordance with the requirements of this policy.

9) A current inventory of wireless technologies and services used on NSS shall be maintained (e.g., number of devices, device model).

10) Guidance for the use of wireless technologies on NSS or in proximity to NSS shall be promulgated throughout the organization.

11) The AO or CSA may terminate wireless network operations in the event of an emergency or security breach.

12) An agreement outlining terms of use shall be signed by each user and system administrator prior to operation (e.g., lost or stolen device reporting requirements).

c. At a minimum, D/As shall implement the following operation control:

   1) Basic education, training (e.g., IA training, use of device or system training, reporting procedures for lost or stolen devices), and awareness regarding the use of wireless technologies connecting to NSS shall be administered to all D/A managers, technical support

personnel, and users of wireless technologies before they can be authorized to operate on wireless NSS. The content of this policy and procedures for its implementation shall be incorporated into training and awareness materials.

d. At a minimum, D/As shall implement the following technical controls:

1) Wireless NSS that transmit, receive, process, or store information shall utilize NSA-approved encryption standards commensurate with the level of information classification as defined in CNSS Policy No. 15, *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems* (Reference m).

2) Confidentiality, integrity, and availability controls, as well as authentication and non-repudiation measures on wireless information systems, shall be in accordance with Reference e and CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems* (Reference n).

3) Authentication employing the Extensible Authentication Protocol (EAP) shall implement cryptographic modules validated under the NIST Cryptographic Module Validation Program commensurate with the level of risk. At a minimum, EAP-Transport Layer Security (EAP-TLS) shall be employed.

4) Wireless and wired intrusion detection systems shall be used to monitor for unauthorized access to the network and to detect malicious wireless activities and the insider threat. Response actions shall take place in accordance with D/A policy.

SECTION V – RESPONSIBILITIES

7. Heads of D/A shall:

a. Ensure resource adequacy to:

1) Maintain a staff of cleared personnel with current credentials and adequate training to NSS programs employing wireless technologies; and

2) Operate, protect, and maintain NSS with wireless capabilities in accordance with this policy.

b. Ensure D/A continuous monitoring under this policy is conducted in accordance with applicable federal laws, in particular those protecting US persons privacy rights.

SECTION VI – DEFINITIONS

8. Cognizant Security Authority (CSA) – The single principal designated by a Senior Official of the D/A to serve as the responsible official for all aspects of security program management concerning the protection of NSS under the D/A's responsibility. For information systems this may be the Authorizing Official (AO).

Note: Within an organization, there may be a hierarchy of cognizant security officers/authorities existing at a variety of echelons (e.g., a specific geographical area, a specific military base or activity) with each CSA having sole jurisdiction within that area or activity.

9. Non-Operational Network – A network that does not store credentials used to login to a NSS network or information system, is not configured to process or store electronic mail (email) from an NSS electronic messaging system, and is not centrally controlled or monitored from an NSS network.

10. Wireless System –Components of a computer network which include at least one device enabled with wireless technology which interconnects with other components to store, process, receive, or send data or information to a wireless enabled mobile device.

11. Terms defined in CNSS Instruction No. 4009: *National Information Assurance Glossary,* (Reference d), apply to this policy.

SECTION VII – REFERENCES

12. References for this policy are listed in ANNEX A. Additionally, informational references are provided in ANNEX B to assist D/As in establishing a wireless communications program for NSS or incorporating wireless communications guidelines into an existing NSS program.

Encl:
ANNEX A - References
ANNEX B – Standards and Best Practices

ANNEX A

REFERENCES

a. CNSS Directive No. 900, *Governing Procedures of the Committee on National Security Systems (CNSS)*, dated May 2013.

b. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, dated July 5, 1990.

c. Executive Order (EO) 12333, *United States Intelligence Activities*, dated December 1981, as amended.

d. CNSS Instruction No. 4009, *National Information Assurance (IA) Glossary*, dated April 2010.

e. CNSSP No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, dated June 2013.

f. CNSSP No. 300, *National Policy on Control of Compromising Emanations*, dated April 2004.

g. CNSS Instruction No. 7000, *Tempest Countermeasures for Facilities*, dated May 2004.

h. CNSS Policy No. 22, *Information Assurance Risk Management Policy for National Security Systems*, dated January 2012.

i. National Security Decision Directive 298, *National Operations Security Program*, dated January 22, 1988.

j. CNSS Directive No. 505, *Supply Chain Risk Management (SCRM)*, dated March 2012.

k. NIST SP 800-147, *BIOS Protection Guidelines*, dated April 2011.

l. NIST SP 800-164 DRAFT, *Guidelines on Hardware-Rooted Security in Mobile Devices*, dated 31 Oct 2012.

m. CNSS Policy No. 15, *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*, dated March 2010.

n. CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, dated March 2012.

ANNEX B

STANDARDS AND BEST PRACTICES

Federal guidelines that articulate best practices, but are not specifically addressed in this policy, are included here for informational purposes:

a. Defense Information Systems Agency, *Wireless Security Technical Implementation Guide Version 6, Release 7*, dated July 26, 2013.

b. Intelligence Community Standard 705-01, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities*, dated September 17, 2010.

c. Intelligence Community Secure Wireless Mobility Framework, version 1.0, dated 30 January 2013.

d. National Institute of Standards and Technology Special Publication (NIST SP) 800-30, G*uide to Conducting Risk Assessments Rev 1*, dated September 2012.

e. NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, dated February 2010.

f. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, dated March 2011.

g. NIST SP 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security*, dated June 2009.

h. NIST SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, dated July 2008.

i. NIST SP 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, dated April 2013.

j. NIST SP 800-63 Revision 1, *Electronic Authentication Guideline*, dated December 2011.

k. NIST SP 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*, dated October 2008.

l. NIST SP 800-97, *Establishing Robust Security Networks: A Guide to IEEE 802.11i*, dated February 2007.

m. NIST SP 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, dated April 2007.

n. NIST SP 800-121, *Guide to Bluetooth Security Rev 1*, dated June 2012.

o. NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*, dated October 2008.

p. NIST SP 800-127, *Guide to Securing WiMAX Wireless Communications*, dated September 2010.

q. NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, dated February 2012.